

APPENDIX A

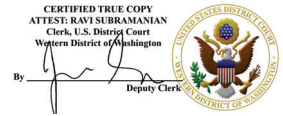
Defendant's Motion to Suppress Evidence and Memorandum in Support of Suppression

United States v. Curcio, 24-CR-312

UNITED STATES DISTRICT COURT

for the

Western District of Washington



In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address)

11512 158th Avenue NE, Redmond, WA 98052, as described more particularly in Attachment A

Case No. MJ24-309

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

11512 158th Avenue NE, Redmond, WA 98052, as described more particularly in Attachment A.

located in the _____ Western _____ District of _____ Washington _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. §§ 1349, 1343, and 2 wire fraud conspiracy, wire fraud, and aiding and abetting the same.

The application is based on these facts:

- ☒ See Affidavit of Special Agent Christopher Campbell, FBI, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Christopher Campbell, Special Agent FBI

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
- ☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 05/22/2024

Judge's signature

City and state: Seattle, Washington

Michelle L. Peterson, United States Magistrate Judge

Printed name and title

1 described in Attachment B to this Affidavit, as well as any digital devices or other
2 electronic storage media located therein.

3 3. The facts set forth in this Affidavit are based on my own personal
4 knowledge; knowledge obtained from other individuals during my participation in this
5 investigation, including other law enforcement officers; interviews of cooperating
6 witnesses; review of documents and records related to this investigation; communications
7 with others who have personal knowledge of the events and circumstances described
8 herein; and information gained through my training and experience.

9 4. Because this Affidavit is submitted for the limited purpose of establishing
10 probable cause in support of the application for a search warrant, it does not set forth
11 each and every fact that I or others have learned during the course of this investigation. I
12 have set forth only the facts that I believe are necessary to establish probable cause to
13 believe that evidence, fruits and instrumentalities of violations of Title 18, United States
14 Code, Sections 1349 (wire fraud conspiracy), 1343 (wire fraud), and 2 (aiding and
15 abetting the same) (collectively, the "Subject Offenses") will be found at the SUBJECT
16 PREMISES.

17 THE INVESTIGATION

18 5. As set forth in the criminal Indictment (the "Indictment") that was returned
19 by a grand jury in the Southern District of New York on May 20, 2024, which is
20 incorporated herein by reference, ANTHONY CURCIO, a/k/a "Brendan
21 Wooley" ("Target Subject-1" or "CURCIO"), and IOSIF BONDARCHUK, a/k/a "Joe
22 Bondarchuk" ("Target Subject-2" or "BONDARCHUK") (collectively, the "Target
23 Subjects"), from at least in or about 2022 up to and including in or about May 2024,
24 engaged in a fraudulent scheme to defraud buyers and marketplaces to purchase sports
25 and Pokémon trading cards at false and inflated prices by misrepresenting that low-to-mid
26 grade cards had received high-grade ratings from a
27

1 reputable card authentication company (“Company-1”), thereby causing victims to pay
 2 more money for the cards than they otherwise would have. In total, the Target Subjects
 3 attempted to deprive victims of over \$2 million through their sales and attempted sales of
 4 trading cards by misrepresenting the grade of numerous trading cards.

5
 6 6. As is further set forth in the Indictment:

- 7 a. Sports and Pokémon trading cards containing the images of professional
 8 athletes and Pokémon can have considerable collectible and resale value
 9 depending on, among other things, their condition and authenticity.
 10 Company-1 is a prominent card authenticator and grader. For a fee,
 11 Company-1 verifies a card’s authenticity, assesses its condition, and
 12 assigns it a numerical grade from one to ten, with one being the lowest
 13 grade and ten being the highest grade. The grade assigned is reflective
 14 of the card’s comparative market value. After grading a card,
 15 Company-1 seals the card in a distinctive, tamper-resistant plastic case
 16 that encloses the card to preserve its condition and indicates its grade on
 17 an affixed label.
- 18 b. The card grade assigned by Company-1 significantly impacts the market
 19 value of the card. As an example, a 1986 Fleer Michael Jordan #57 card
 20 graded as an 8 has an estimated market value of between \$6,000 and
 21 \$7,000. But this same card, when graded as a 10 by Company-1, has
 22 had an estimated market value of between approximately \$185,000 and
 23 \$203,000. In short, representations about Company-1’s grade of the
 24 card go directly to the value of the card itself and the price at which the
 25 card can be bought and sold.
- 26 c. The Target Subjects sold and attempted to sell sports and Pokémon
 27 trading cards through, among other means, an online card marketplace
 based in Manhattan (the “Manhattan Marketplace”). Through the
 Manhattan Marketplace, the Target Subjects sold various cards at
 inflated prices by falsely claiming the cards had been assigned higher
 ratings by Company-1 than was true.
- d. Among the cards that the Target Subjects sold as part of the scheme
 through the Manhattan Marketplace was a 1986 Fleer Michael Jordan
 #57 card (the “1986 MJ Card”). In or about May 2022, CURCIO
 advertised one version of the 1986 MJ Card on the Manhattan
 Marketplace for sale for the amount of \$171,700, as pictured below.



As is depicted above, Target Subject-1 advertised the 1986 MJ Card as having a purported grade of “10” assigned by Company-1. In truth and in fact, Target Subject-1 knew that Company-1 had not assigned this grade to the card. To make it appear that the 1986 MJ Card had received a grade of 10 from Company-1, Target Subject-1 caused the 1986 MJ Card to be displayed in the distinctive, tamper-resistant plastic case of Company-1 with a labeled rating of 10, when, in reality, the 1986 MJ Card he was offering for sale had received no such rating from Company-1. Through this fraudulent scheme, Target Subject-1 made these misrepresentations to fraudulently inflate the card’s value and induce victims to pay more money for the 1986 MJ Card than they otherwise would have paid. To further make it appear that the 1986 MJ Card had received a rating of 10 from Company-1, Target Subject-1

1 caused a purported Company-1 label to be included in the plastic case,
2 along with a fraudulent bar code and certification number.

3 e. During the fraudulent trading card scheme, when victims demanded
4 refunds and confronted the Target Subjects over the misrepresented,
5 fraudulent cards, including by showing the Target Subjects
6 confirmations from Company-1 that the Target Subjects had
7 misrepresented the grade of the cards, the Target Subjects feigned
8 ignorance and often refunded the victims. Yet, after being put on notice
9 that the cards' grades and labels were fraudulent, the Target Subjects
10 repeatedly attempted to, and did, sell these very same cards to
11 subsequent victims, again with fraudulent labels showing an inflated,
12 grade from Company-1.

13 f. The Target Subjects sold and attempted to sell fraudulently
14 misrepresented cards using several different methods, including online
15 sales through the Manhattan Marketplace. The Target Subjects
16 completed at least eight fraudulent sales, totaling \$225,000 in value,
17 through the Manhattan Marketplace. The Target Subjects repeatedly
18 sent a variety of interstate wires into and out of Manhattan in
19 furtherance of the fraud, including posts on the Manhattan
20 Marketplace's website, messages to website administrators, and
21 messages to individual victims through the website's messaging portal.
22 The Target Subjects also sold and attempted to sell fraudulently
23 misrepresented cards at in-person card shops, auctions, and card shows.

24 g. The Target Subjects also fraudulently misrepresented the Company-1
25 grade of Pokémon trading cards to induce victims to pay more money
26 for the cards than they otherwise would have paid. Among the
27 fraudulently misrepresented cards that the Target Subjects sold and
attempted to sell are a 1999 Pokémon Venusaur card and a 1999
Pokémon Charizard card, pictured below.



In or about July 2023, as part of a law enforcement undercover purchase of the above fraudulently misrepresented 1999 Pokémon Venusaur card for \$10,500—which card Target Subject-2 had previously attempted to sell on an online marketplace—Target Subject-1 mailed the card to the undercover law enforcement purchaser at an address in Manhattan after the undercover purchaser wired the money to a bank account that Target Subject-1 controlled.

7. Based on information provided to me and other law enforcement agents by certain victims of the fraudulent trading card scheme, my discussions with other law enforcement agents, my training and experience, and my participation in this investigation, I have learned that Target Subject-1 repeatedly provided the SUBJECT PREMISES as his shipping address to victims. Specifically, when victims learned that the trading cards were fraudulent and demanded refunds and/or otherwise confronted Target Subject-1 about the fraudulent trading cards, among other things, Target Subject-1 asked the victims to return the fraudulent trading cards to him by mailing the cards to the

1 SUBJECT PREMISES. A victim returned a fraudulent card to Target Subject-1 at the
2 TARGET PREMISES as recently as September 2023.

3 8. Based on purchase records produced to law enforcement pursuant to a
4 grand jury subpoena served upon an online marketplace, my discussions with other law
5 enforcement agents, my training and experience, and my participation in this
6 investigation, I have learned that, during the fraudulent trading card scheme, Target
7 Subject-1 ordered various items needed to create forged card cases and labels to be
8 delivered to his listed residence, the SUBJECT PREMISES. Specifically, between in or
9 about June 2022 and in or about February 2024, Target Subject-1 purchased various card
10 grading cases, thermal transfer barcode labels, a magnifier loupe optical glass, a handheld
11 inkjet printer, a lock-cutting kit, an electric grinding pen, an abrasive buffer and polishing
12 wheel, an abrasive and bristle brushes, and drill bits designed for engraving. The most
13 recent purchase, in February 2024, was for drill bits designed for engraving.

14 9. Based on flight records obtained by law enforcement pursuant to a database
15 search, my discussions with other law enforcement agents, my training and experience,
16 and my participation in this investigation, I have learned that Target Subject-1 attended a
17 card show as recently as April 2024, in New Jersey, where he was identified and removed
18 from the show for having fraudulent cards. Target Subject-1 flew directly from Seattle to
19 Newark, New Jersey, to attend this card show.

20 10. Based on records produced to law enforcement pursuant to grand jury
21 subpoenas served upon phone companies and financial institutions, my discussions with
22 other law enforcement agents, my training and experience, and my participation in this
23 investigation, I have learned that the SUBJECT PREMISES are listed as Target Subject-
24 1's address on Target Subject-1's driver's license and bank records. Target Subject-1
25 lives with his wife and two children at the SUBJECT PREMISES. Surveillance was
26 conducted on the SUBJECT PREMISES on multiple days in May 2024. As recently as
27 May 21, 2024, the Target Subject-1 was viewed at the SUBJECT PREMISES.

11. As is described above and in the Indictment, it appears that Target Subject-1 used the SUBJECT PREMISES to further the fraudulent trading card scheme. Based on my training and experience and my participation in this investigation, including my review of Target Subject-1's communications with victims, there is probable cause to believe that the SUBJECT PREMISES will include, among other things, fraudulent trading cards and certain tools and equipment needed to create forged card cases and labels in connection with the commission of the Subject Offenses.

12. Based on my training and experience, I know that individuals who engage in the Subject Offenses routinely store the proceeds of their crimes in their residences. In addition, I know that within their residences, individuals who engage in the Subject Offenses often store the proceeds of their crimes in safes, key-lock strong boxes, suitcases, locked cabinets, and other types of locked or closed containers. I therefore seek authorization to open any closed items and containers or to seize any such closed items and containers so that they may be opened if tools or other implements are required.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

13. As described above and in Attachment B, this application seeks permission to search for evidence, fruits and/or instrumentalities that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the evidence, fruits, and/or instrumentalities might be found is data stored on digital devices¹

¹ "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

1 such as computer hard drives or other electronic storage media.² Thus, the warrant
2 applied for would authorize the seizure of digital devices or other electronic storage
3 media or, potentially, the copying of electronically stored information from digital
4 devices or other electronic storage media, all under Rule 41(e)(2)(B).

5 14. *Probable cause.* Based upon my review of the evidence gathered in this
6 investigation, my review of data and records, information received from other agents and
7 computer forensics examiners, and my training and experience, I submit that if a digital
8 device or other electronic storage media is found at the SUBJECT PREMISES, there is
9 probable cause to believe that evidence, fruits, and/or instrumentalities of the Subject
10 Offenses will be stored on those digital devices or other electronic storage media.

11 15. Based on information provided to me and other law enforcement agents by
12 certain victims of the fraudulent trading card scheme, my discussions with other law
13 enforcement agents, my training and experience, and my participation in this
14 investigation, I have learned that Target Subject-1 uses electronic devices to
15 communicate with victims. Specifically, based on the foregoing, I know that Target
16 Subject-1 communicated with victims via emails, phone calls, and text messages.

17 16. Based on my training and experience, I know that individuals who engage
18 in the Subject Offenses commonly use cellphones and other electronic devices to
19 communicate in furtherance of their criminal scheme, including by using email, text
20 messages, messaging applications, and voice calls to communicate with any co-
21 conspirators or aiders or abettors and victims. Indeed, as stated above, during the course
22 of this investigation, I have reviewed electronic communications of Target Subject-1 with
23 certain victims of the Subject Offenses that occurred by email and text message. Based
24 on my training and experience, I know that individuals who engage in fraud schemes

25 _____
26 ² Electronic Storage media is any physical object upon which electronically stored
27 information can be recorded. Examples include hard disks, RAM, floppy disks, flash
memory, CD-ROMs, and other magnetic or optical media.

1 often store data on their cellphones related to their illegal activity, which can include logs
2 of online “chats” with co-conspirators and victims; email and other electronic
3 correspondence with co-conspirators and victims; contact information of co-conspirators
4 and victims, including telephone numbers, email addresses, and identifiers for instant
5 messaging and social medial accounts; and records of the disposition of criminal
6 proceeds, among other things.

7 17. Based on my training, experience, and research, I know that while
8 cellphones and smartphones both have voice call and messaging capabilities,
9 smartphones also have capabilities that allow them to serve as a wireless telephone,
10 digital camera, internet-capable device, and GPS navigation device, among other things.
11 Accordingly, cellphones and smartphones often contain information such as contact lists
12 (including phone numbers) and text and photo messages. Smartphones also often contain
13 photos, internet-browsing history, GPS information, and messaging content.

14 18. Based on the foregoing, there is probable cause to believe that evidence,
15 fruits and/or instrumentalities of the Subject Offenses exists and will be found on digital
16 device or other electronic storage media at the SUBJECT PREMISES, for at least the
17 following reasons:

- 18 a. Based on my knowledge, training, and experience, I know that computer
19 files or remnants of such files can be preserved (and consequently also then
20 recovered) for months or even years after they have been downloaded onto
21 a storage medium, deleted, or accessed or viewed via the Internet.
22 Electronic files downloaded to a digital device or other electronic storage
23 medium can be stored for years at little or no cost. Even when files have
24 been deleted, they can be recovered months or years later using forensic
25 tools. This is so because when a person “deletes” a file on a digital device
26 or other electronic storage media, the data contained in the file does not
27 actually disappear; rather, that data remains on the storage medium until it
is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free
space or slack space—that is, in space on the digital device or other
electronic storage medium that is not currently being used by an active

1 file—for long periods of time before they are overwritten. In addition, a
2 computer’s operating system may also keep a record of deleted data in a
“swap” or “recovery” file.

- 3 c. Wholly apart from user-generated files, computer storage media—in
4 particular, computers’ internal hard drives—contain electronic evidence of
5 how a computer has been used, what it has been used for, and who has used
6 it. To give a few examples, this forensic evidence can take the form of
7 operating system configurations, artifacts from operating system or
8 application operation; file system data structures, and virtual memory
“swap” or paging files. Computer users typically do not erase or delete this
evidence, because special software is typically required for that task.
However, it is technically possible to delete this information.
- 9 d. Similarly, files that have been viewed via the Internet are sometimes
10 automatically downloaded into a temporary Internet directory or “cache.”

11 19. *Forensic evidence.* As further described in Attachment B, this application
12 seeks permission to locate not only computer files that might serve as direct evidence of
13 the crimes described on the warrant, but also for forensic electronic evidence that
14 establishes how digital devices or other electronic storage media were used, the purpose
15 of their use, who used them, and when. There is probable cause to believe that this
16 forensic electronic evidence will be on any digital devices or other electronic storage
17 media located at the SUBJECT PREMISES because:

- 18 a. Stored data can provide evidence of a file that was once on the digital
19 device or other electronic storage media but has since been deleted or edited, or
20 of a deleted portion of a file (such as a paragraph that has been deleted from a
21 word processing file). Virtual memory paging systems can leave traces of
22 information on the digital device or other electronic storage media that show
23 what tasks and processes were recently active. Web browsers, e-mail
24 programs, and chat programs store configuration information that can reveal
25 information such as online nicknames and passwords. Operating systems can
26 record additional information, such as the history of connections to other
27 computers, the attachment of peripherals, the attachment of USB flash storage
devices or other external storage media, and the times the digital device or
other electronic storage media was in use. Computer file systems can record
information about the dates files were created and the sequence in which they
were created.

1 b. As explained herein, information stored within a computer and other
2 electronic storage media may provide crucial evidence of the “who, what, why,
3 when, where, and how” of the criminal conduct under investigation, thus
4 enabling the United States to establish and prove each element or alternatively,
5 to exclude the innocent from further suspicion. In my training and experience,
6 information stored within a computer or storage media (e.g., registry
7 information, communications, images and movies, transactional information,
8 records of session times and durations, internet history, and anti-virus,
9 spyware, and malware detection programs) can indicate who has used or
10 controlled the computer or storage media. This “user attribution” evidence is
11 analogous to the search for “indicia of occupancy” while executing a search
12 warrant at a residence. The existence or absence of anti-virus, spyware, and
13 malware detection programs may indicate whether the computer was remotely
14 accessed, thus inculcating or exculpating the computer owner and/or others
15 with direct physical access to the computer. Further, computer and storage
16 media activity can indicate how and when the computer or storage media was
17 accessed or used. For example, as described herein, computers typically
18 contain information that log: computer user account session times and
19 durations, computer activity associated with user accounts, electronic storage
20 media that connected with the computer, and the IP addresses through which
21 the computer accessed networks and the internet. Such information allows
22 investigators to understand the chronological context of computer or electronic
23 storage media access, use, and events relating to the crime under
24 investigation.¹ Additionally, some information stored within a computer or
25 electronic storage media may provide crucial evidence relating to the physical
26 location of other evidence and the suspect. For example, images stored on a
27 computer may both show a particular location and have geolocation
information incorporated into its file data. Such file data typically also
contains information indicating when the file or image was created. The
existence of such image files, along with external device connection logs, may
also indicate the presence of additional electronic storage media (e.g., a digital
camera or cellular phone with an incorporated camera). The geographic and
timeline information described herein may either inculcate or exculpate the
computer user. Last, information stored within a computer may provide
relevant insight into the computer user’s state of mind as it relates to the
offense under investigation. For example, information within the computer
may indicate the owner’s motive and intent to commit a crime (e.g., internet
searches indicating criminal planning), or consciousness of guilt (e.g., running

¹ For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

1 a “wiping” program to destroy evidence on the computer or password
2 protecting/encrypting such evidence in an effort to conceal it from law
enforcement).

3 c. A person with appropriate familiarity with how a digital device or other
4 electronic storage media works can, after examining this forensic evidence in
5 its proper context, draw conclusions about how the digital device or other
6 electronic storage media were used, the purpose of their use, who used them,
and when.

7 d. The process of identifying the exact files, blocks, registry entries, logs, or
8 other forms of forensic evidence on a digital device or other electronic storage
9 media that are necessary to draw an accurate conclusion is a dynamic process.
10 While it is possible to specify in advance the records to be sought, digital
11 evidence is not always data that can be merely reviewed by a review team and
12 passed along to investigators. Whether data stored on a computer is evidence
may depend on other information stored on the computer and the application of
knowledge about how a computer behaves. Therefore, contextual information
necessary to understand other evidence also falls within the scope of the
warrant.

13 e. Further, in finding evidence of how a digital device or other electronic
14 storage media was used, the purpose of its use, who used it, and when,
15 sometimes it is necessary to establish that a particular thing is not present. For
16 example, the presence or absence of counter-forensic programs or anti-virus
programs (and associated data) may be relevant to establishing the user’s
intent.

17 **DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES**

18 20. There is probable cause to believe that the SUBJECT PREMISES contains
19 electronic, digital devices that contain evidence, fruits and instrumentalities of the
20 Subject Offenses. In particular, based on information provided to me and other law
21 enforcement agents by certain victims of the fraudulent trading card scheme, my
22 discussions with other law enforcement agents, my training and experience, and my
23 participation in this investigation, I have learned that Target Subject-1 uses electronic
24 devices to communicate with victims of the Subject Offenses. Specifically, based on the
25
26
27

1 foregoing, I know that Target Subject-1 communicated with victims via emails, phone
2 calls, and text messages.

3 a. In particular, there is probable cause to believe that electronic devices in the
4 SUBJECT PREMISES contain email communications concerning the Subject
5 Offenses. For instance, Target Subject-1's laptop and smartphone are likely to
6 contain emails about the exchange of trading cards for money or other trading
7 cards given that, as recently as April 2024, a victim exchanged such emails
8 with Target Subject-1.

9 b. Moreover, there is probable cause to believe that electronic devices in the
10 SUBJECT PREMISES contain logs of phone calls relating to the Subject
11 Offenses. For instance, Target Subject-1's cellphone is likely to contain such
12 evidence because, in connection with this investigation, law enforcement has
13 obtained an audio recording of a call between Target Subject-1 and a particular
14 victim concerning the Subject Offenses.

15 c. Finally, there is probable cause to believe that cellphones and smartphones
16 in the SUBJECT PREMISES contain text messages concerning the Subject
17 Offenses. For instance, Target Subject-1's cellphones are likely to contain text
18 messages concerning the return and refund of certain fraudulent trading cards
19 because, in connection with this investigation, law enforcement has obtained
20 text messages with certain victims that show Target Subject-1 directing the
21 victims to return the fraudulent trading cards to him by mailing the cards to the
22 SUBJECT PREMISES.

23 21. Based on my training and experience, I know that individuals who engage
24 in the Subject Offenses commonly use cellphones and other electronic devices to
25 communicate in furtherance of their criminal scheme, including by using email, text
26 messages, messaging applications, and voice calls to communicate with any co-
27 conspirators or aiders or abettors and victims. Indeed, as stated above, during the course
of this investigation, I have reviewed electronic communications of Target Subject-1 with
certain victims of the Subject Offenses that occurred by email and text message. Based
on my training and experience, I know that individuals who engage in fraud schemes
often store data on their cellphones related to their illegal activity, which can include logs
of online "chats" with co-conspirators and victims; email and other electronic
correspondence with co-conspirators and victims; contact information of co-conspirators

1 and victims, including telephone numbers, email addresses, and identifiers for instant
2 messaging and social medial accounts; and records of the disposition of criminal
3 proceeds, among other things.

4 22. Based on my training, experience, and research, I know that while
5 cellphones and smartphones both have voice call and messaging capabilities,
6 smartphones also have capabilities that allow them to serve as a wireless telephone,
7 digital camera, internet-capable device, and GPS navigation device, among other things.
8 Accordingly, cellphones and smartphones often contain information such as contact lists
9 (including phone numbers) and text and photo messages. Smartphones also often contain
10 photos, internet-browsing history, GPS information, and messaging content.

11 23. Because of the nature of the evidence that I am attempting to obtain and the
12 nature of the investigation, I have not made any prior efforts to obtain the evidence based
13 on the consent of any party who may have authority to consent. I believe, based upon the
14 nature of the investigation and the information I have received, that if Target Subject-1
15 becomes aware of the investigation in advance of the execution of a search warrant, he
16 may attempt to destroy any potential evidence, whether digital or non-digital, thereby
17 hindering law enforcement agents from the furtherance of the criminal investigation.

18
19 **REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF TARGET**
20 **COMPUTERS**

21 24. *Necessity of seizing or copying entire computers or storage media.* In most
22 cases, a thorough search of premises for information that might be stored on digital
23 devices or other electronic storage media often requires the seizure of the physical items
24 and later off-site review consistent with the warrant. In lieu of removing all of these
25 items from the premises, it is sometimes possible to make an image copy of the data on
26 the digital devices or other electronic storage media, onsite. Generally speaking, imaging
27 is the taking of a complete electronic picture of the device's data, including all hidden

1 sectors and deleted files. Either seizure or imaging is often necessary to ensure the
2 accuracy and completeness of data recorded on the item, and to prevent the loss of the
3 data either from accidental or intentional destruction. This is true because of the
4 following:

5 a. *The time required for an examination.* As noted above, not all evidence
6 takes the form of documents and files that can be easily viewed on site.
7 Analyzing evidence of how a computer has been used, what it has been used
8 for, and who has used it requires considerable time, and taking that much time
9 on premises could be unreasonable. As explained above, because the warrant
10 calls for forensic electronic evidence, it is exceedingly likely that it will be
11 necessary to thoroughly examine the respective digital device and/or electronic
12 storage media to obtain evidence. Computer hard drives, digital devices and
13 electronic storage media can store a large volume of information. Reviewing
14 that information for things described in the warrant can take weeks or months,
15 depending on the volume of data stored, and would be impractical and invasive
16 to attempt on-site.

17 b. *Technical requirements.* Digital devices or other electronic storage media
18 can be configured in several different ways, featuring a variety of different
19 operating systems, application software, and configurations. Therefore,
20 searching them sometimes requires tools or knowledge that might not be
21 present on the search site. The vast array of computer hardware and software
22 available makes it difficult to know before a search what tools or knowledge
23 will be required to analyze the system and its data on the premises. However,
24 taking the items off-site and reviewing them in a controlled environment will
25 allow examination with the proper tools and knowledge.

26 c. *Variety of forms of electronic media.* Records sought under this warrant
27 could be stored in a variety of electronic storage media formats and on a
variety of digital devices that may require off-site reviewing with specialized
forensic tools.

REQUEST FOR AUTHORITY TO OBTAIN PHYSICAL BIOMETRIC **CHARACTERISTICS**

25 25. The warrant I am applying for would permit law enforcement to obtain
26 from certain individuals the display of physical biometric characteristics (such as
27 fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to

1 search and seizure pursuant to this warrant. I seek this authority based on the
2 following:

3 a. I know from my training and experience, as well as from information found
4 in publicly available materials published by device manufacturers, that many
5 electronic devices, particularly newer mobile devices and laptops, offer their
6 users the ability to unlock the device through biometric features in lieu of a
7 numeric or alphanumeric passcode or password. These biometric features
8 include fingerprint scanners and facial recognition features. Some devices offer
9 a combination of these biometric features, and the user of such devices can
10 select which features they would like to utilize.

11 b. If a device is equipped with a fingerprint scanner, a user may enable the
12 ability to unlock the device through his or her fingerprints. For example, Apple
13 offers a feature called "Touch ID," which allows a user to register up to five
14 fingerprints that can unlock a device. Once a fingerprint is registered, a user
15 can unlock the device by pressing the relevant finger to the device's Touch ID
16 sensor, which is found in the round button (often referred to as the "home"
17 button) located at the bottom center of the front of the device. The fingerprint
18 sensors found on devices produced by other manufacturers have different
19 names but operate similarly to Touch ID.

20 c. If a device is equipped with a facial recognition feature, a user may enable
21 the ability to unlock the device through his or her face, iris, or retina. For
22 example, Apple offers a facial recognition feature called "Face ID." During
23 the Face ID registration process, the user holds the device in front of his or her
24 face. The device's camera then analyzes and records data based on the user's
25 facial characteristics. The device can then be unlocked if the camera detects a
26 face with characteristics that match those of the registered face. Facial
27 recognition features found on devices produced by other manufacturers have
different names but operate similarly to Face ID.

d. While not as prolific on digital devices as fingerprint and facial-recognition
features, both iris and retina scanning features exist for securing devices/data.
The human iris, like a fingerprint, contains complex patterns that are unique
and stable. Iris recognition technology uses mathematical pattern-recognition
techniques to map the iris using infrared light. Similarly, retina scanning casts
infrared light into a person's eye to map the unique variations of a person's
retinal blood vessels. A user can register one or both eyes to be used to unlock
a device with these features. To activate the feature, the user holds the device
in front of his or her face while the device directs an infrared light toward the
user's face and activates an infrared sensitive camera to record data from the
person's eyes. The device is then unlocked if the camera detects the registered
eye.

1 e. In my training and experience, users of electronic devices often enable the
2 aforementioned biometric features because they are considered to be a more
3 convenient way to unlock a device than by entering a numeric or alphanumeric
4 passcode or password. Moreover, in some instances, biometric features are
5 considered to be a more secure way to protect a device's contents. This is
6 particularly true when the users of a device are engaged in criminal activities
7 and thus have a heightened concern about securing the contents of a device.

8 f. As discussed in this affidavit, based on my training and experience I
9 believe that one or more digital devices will be found during the search. The
10 passcode or password that would unlock the device(s) subject to search under
11 this warrant is not known to law enforcement. Thus, law enforcement
12 personnel may not otherwise be able to access the data contained within the
13 device(s), making the use of biometric features necessary to the execution of
14 the search authorized by this warrant.

15 g. I also know from my training and experience, as well as from information
16 found in publicly available materials including those published by device
17 manufacturers, that biometric features will not unlock a device in some
18 circumstances even if such features are enabled. This can occur when a device
19 has been restarted, inactive, or has not been unlocked for a certain period of
20 time. For example, Apple devices cannot be unlocked using Touch ID when
21 (1) more than 48 hours has elapsed since the device was last unlocked or (2)
22 when the device has not been unlocked using a fingerprint for 4 hours *and* the
23 passcode or password has not been entered in the last 156 hours. Biometric
24 features from other brands carry similar restrictions. Thus, in the event law
25 enforcement personnel encounter a locked device equipped with biometric
26 features, the opportunity to unlock the device through a biometric feature may
27 exist for only a short time.

h. In my training and experience, the person who is in possession of a device
or has the device among his or her belongings at the time the device is found is
likely a user of the device. However, in my training and experience, that person
may not be the only user of the device, and may not be the only individual
whose physical characteristics are among those that will unlock the device via
biometric features. Furthermore, while physical proximity is an important
factor in determining who is the user of a device, it is only one among many
other factors that may exist.

i. Due to the foregoing, I request that if law enforcement personnel encounter
a device that is subject to search and seizure pursuant to this warrant and may
be unlocked using one of the aforementioned biometric features, and if law
enforcement reasonably suspects ANTHONY CURCIO is a user of the device,
then – for the purpose of attempting to unlock the device in order to search the

1 contents as authorized by this warrant – law enforcement personnel shall be
2 authorized to: (1) press or swipe the fingers (including thumbs) of CURCIO to
3 the fingerprint scanner of the device; and/or (2) hold the device in front of the
4 face and open eyes of CURCIO and activate the facial, iris, or retina
5 recognition feature.

6 j. In pressing or swiping an individual's thumb or finger onto a device and in
7 holding a device in front of an individual's face and open eyes, law
8 enforcement may not use excessive force, as defined in *Graham v. Connor*,
9 490 U.S. 386 (1989); specifically, law enforcement may use no more than
10 objectively reasonable force in light of the facts and circumstances confronting
11 them.

12 SEARCH TECHNIQUES

13 26. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal
14 Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging,
15 or otherwise copying digital devices or other electronic storage media that reasonably
16 appear capable of containing some or all of the data or items that fall within the scope of
17 Attachment B to this Affidavit, and will specifically authorize a later review of the media
18 or information consistent with the warrant.

19 27. Because several people share the SUBJECT PREMISES as a residence, it is
20 possible that the SUBJECT PREMISES will contain digital devices or other electronic
21 storage media that are predominantly used, and perhaps owned, by persons who are not
22 suspected of a crime. If agents conducting the search nonetheless reasonably suspect that
23 the things described in this warrant could be found on those computers, this application
24 seeks permission to search and if necessary to seize those computers as well. It may be
25 impossible to determine, on scene, which computers contain the things described in this
26 warrant.

27 28. Consistent with the above, I hereby request the Court's permission to seize
and/or obtain a forensic image of digital devices or other electronic storage media that
reasonably appear capable of containing data or items that fall within the scope of

Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or other electronic storage media and/or forensic images, using the following procedures:

A. Processing the Search Sites and Securing the Data.

a. Upon securing the physical search site, the search team will conduct an initial review of any digital devices or other electronic storage media located at the subject premises described in Attachment A that are capable of containing data or items that fall within the scope of Attachment B to this Affidavit, to determine if it is possible to secure the data contained on these devices onsite in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. In order to examine the electronically stored information (“ESI”) in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of any digital device or other electronic storage media that is capable of containing data or items that fall within the scope of Attachment B to this Affidavit.³

c. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one physical hard drive). Therefore, creating an image of a logical drive does not include every bit and byte on the physical drive. Law enforcement will only create an image of physical or logical drives physically present on or within the subject device. Creating an image of the devices located at the search locations described in Attachment A

³ The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

1 will not result in access to any data physically located elsewhere. However,
2 digital devices or other electronic storage media at the search locations
3 described in Attachment A that have previously connected to devices at other
locations may contain data from those other locations.

4 d. If based on their training and experience, and the resources available to
5 them at the search site, the search team determines it is not practical to make an
6 on-site image within a reasonable amount of time and without jeopardizing the
7 ability to accurately preserve the data, then the digital devices or other
electronic storage media will be seized and transported to an appropriate law
enforcement laboratory to be forensically imaged and reviewed.

8 **B. Searching the Forensic Images.**

9 a. Searching the forensic images for the items described in Attachment B may
10 require a range of data analysis techniques. In some cases, it is possible for
11 agents and analysts to conduct carefully targeted searches that can locate
12 evidence without requiring a time-consuming manual search through unrelated
13 materials that may be commingled with criminal evidence. In other cases,
14 however, such techniques may not yield the evidence described in the warrant,
15 and law enforcement may need to conduct more extensive searches to locate
16 evidence that falls within the scope of the warrant. The search techniques that
17 will be used will be only those methodologies, techniques and protocols as
18 may reasonably be expected to find, identify, segregate and/or duplicate the
19 items authorized to be seized pursuant to Attachment B to this affidavit. Those
20 techniques, however, may necessarily expose many or all parts of a hard drive
21 to human inspection in order to determine whether it contains evidence
22 described by the warrant.

19 **CONCLUSION**

20 29. Based on the foregoing, I believe there is probable cause that evidence,
21 fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1349
22 (wire fraud conspiracy), 1343 (wire fraud), and 2 (aiding and abetting the same) are
23 located at the SUBJECT PREMISES, as more fully described in Attachment A to this
24 Affidavit, as well as on and in any digital devices or other electronic storage media found
25 at the SUBJECT PREMISES. I therefore request that the court issue a warrant
26 authorizing a search of the SUBJECT PREMISES, as well as any digital devices and
27

1 electronic storage media located therein, for the items more fully described in Attachment
2 B hereto, incorporated herein by reference, and the seizure of any such items found
3 therein.

4 30. The affidavit and application are being presented by reliable electronic
5 means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).

6
7
8 
9 CHRISTOPHER CAMPBELL
Special Agent
Federal Bureau of Investigation

10
11 The above-named agent provided a sworn statement to the truth of the foregoing
12 affidavit by telephone on the 22nd day of May, 2024.
13

14
15 
16 MICHELLE L. PETERSON
United States Magistrate Judge
17
18
19
20
21
22
23
24
25
26
27

ATTACHMENT A

The property to be searched is 11512 158th Ave NE, Redmond, WA 98052, further described as multi-story, single-family home, and any digital devices or other electronic storage media found therein. The street view and side view of the SUBJECT PREMISES are depicted in the following photographs:



ATTACHMENT B
ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. §§ 1349 (wire fraud conspiracy), 1343 (wire fraud), and 2 (aiding and abetting the same) (collectively, the “Subject Offenses”) involving Target Subject-1, ANTHONY CURCIO:

1. Evidence concerning occupancy or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys;

2. Trading cards and Pokémon cards located within the SUBJECT PREMISES;

3. Any tools, materials, and/or equipment that may be used to create forged card cases and labels;

4. For the time period of January 1, 2022 to the present, evidence relating to the Target Subjects communicating with victims, with each other, and with co-conspirators;

5. For the period of January 1, 2022 to the present, evidence of communications constituting or discussing or regarding the commission of the Subject Offenses;

6. Evidence concerning the identities and locations of co-conspirators and victims;

7. Evidence of criminal conduct, including communications reflecting an agreement between the Target Subjects and other co-conspirators to engage in the

1 scheme to defraud customers who purchased cards from the Target Subjects and their
2 co-conspirators;

3 8. Proceeds of the commission of the Subject Offenses, including any bulk
4 cash contained within the SUBJECT PREMISES;

5 9. Evidence of the use of aliases by the Target Subjects, including documents
6 reflecting false names;

7 10. Evidence relating to state of mind, including communications relating to
8 the Target Subjects' understanding that certain representations being made to
9 individuals purchasing cards from them were or must have been false;

10 11. For the time period of January 1, 2022 to the present, evidence of the
11 receipt, transfer, disposition or location of funds derived from the commission of the
12 Subject Offenses;

13 12. Records of Internet activity, including firewall logs, caches, browser history
14 and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered
15 into any Internet search engine, and records of user-typed web addresses;

16 13. Evidence of user attribution showing who used or owned an electronic
17 device at the time the things described in this warrant were created, edited, or deleted,
18 such as logs, phonebooks, saved usernames and passwords, documents, and browsing
19 history;

20 14. Any items or records needed to access the data stored on any seized or
21 copied electronic devices or storage media, including but not limited to any encryption
22 devices, or records of login credentials, passwords, private encryption keys, or similar
23 information;

24 15. Any items or records that may facilitate a forensic examination of
25 electronic devices or storage media, including any hardware or software manuals or
26 other information concerning the configuration of the seized or copied electronic
27 devices or storage media;

16. Location data, including but not limited to geolocation reporting and
location history data and metadata associated with other files that would place the
Target Subjects and any co-conspirators and/or aiders and abettors, as well as the
devices they used, in specific places at specific times, and would indicate the use of
their devices during those times;

17. Safes, key-lock strong boxes, suitcases, locked cabinets, and other types of
locked or closed containers used to secrete and store currency, electronic devices,
identification documents, books, records, financial instruments, and other and other

1 items within the categories described herein. Law enforcement agents executing this
 2 warrant are specifically authorized to open any such locked safes or containers
 3 including, where necessary, by using reasonable force. Law enforcement agents shall
 4 not seize locked safes or containers that do not contain evidence or fruits of the Subject
 5 Offenses, unless the safes or containers cannot be opened using reasonable force at the
 6 SUBJECT PREMISES. Any locked safe or container that can only be opened away
 7 from the SUBJECT PREMISES shall be returned if a later search shows that it does
 8 not contain evidence or fruits of the Subject Offenses;

9 18. Evidence concerning the location of other evidence of the Subject Offenses,
 10 including but not limited to information concerning addresses of other premises
 11 potentially containing relevant evidence, financial accounts where criminal proceeds
 12 may be stored, and communications reflecting registration of online accounts
 13 potentially containing relevant evidence;

14 19. Digital devices² or other electronic storage media³ that law enforcement
 15 reasonably suspects belong to Target Subject-1, ANTHONY CURCIO, containing any
 16 of the records or information described above or used as a means to commit the
 17 violations described above, including to generate, store, or transmit records in
 18 furtherance of the violations.

19 20. For any digital device or other electronic storage media upon which
 20 electronically stored information that is called for by this warrant may be contained,
 21 that may contain things otherwise called for by this warrant, or whose seizure is
 22 otherwise authorized by this warrant:

23 a. evidence of who used, owned, or controlled the digital device or
 24 other electronic storage media at the time the things described in this warrant were
 25 created, edited, or deleted, such as logs, registry entries, configuration files, saved
 26 usernames and passwords, documents, browsing history, user profiles, email, email
 27 contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital
 device or other electronic storage media, such as viruses, Trojan horses, and other forms

² "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

³ Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1 of malicious software, as well as evidence of the presence or absence of security software
2 designed to detect malicious software;

3 c. evidence of the lack of such malicious software;

4 d. evidence of the attachment to the digital device of other storage
5 devices or similar containers for electronic evidence;

6 e. evidence of counter-forensic programs (and associated data) that are
7 designed to eliminate data from the digital device or other electronic storage media;

8 f. evidence of the times the digital device or other electronic storage
9 media was used;

10 g. physical keys, encryption devices, dongles and similar physical
11 items that are necessary to gain access to the computer equipment, storage devices or
12 data; and

13 h. passwords, password files, test keys, encryption codes or other
14 information necessary to access the computer equipment, storage devices or data.

15 i. documentation and manuals that may be necessary to access the
16 digital device or other electronic storage media or to conduct a forensic examination of
17 the digital device or other electronic storage media;

18 j. applications, utility programs, compilers, interpreters, and other
19 software used to facilitate direct or indirect communication with the computer hardware,
20 storage devices, or data to be searched;

21 k. contextual information necessary to understand the evidence
22 described in this attachment.

23 THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE
24 MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS
25 SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO
26 THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC
27 STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL
ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE
CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR

1 EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED
2 CRIMES.

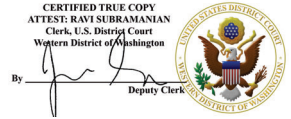
3 During the execution of the search of the SUBJECT PREMISES described in
4 Attachment A, if law enforcement encounters a smartphone or other electronic device
5 equipped with a biometric-unlock feature, and if law enforcement reasonably suspects
6 ANTHONY CURCIO is a user of the device, then – for the purpose of attempting to
7 unlock the device in order to search the contents as authorized by this warrant – law
8 enforcement personnel are authorized to: (1) press or swipe the fingers (including
9 thumbs) of CURCIO to the fingerprint scanner of the device; and/or (2) hold the device
10 in front of the face and open the eyes of CURCIO and activate the facial, iris, or retina
11 recognition feature.

12 In pressing or swiping an individual's thumb or finger onto a device and in
13 holding a device in front of an individual's face and open eyes, law enforcement may not
14 use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically,
15 law enforcement may use no more than objectively reasonable force in light of the facts
16 and circumstances confronting them.

17
18
19
20
21
22
23
24
25
26
27

UNITED STATES DISTRICT COURT

for the
Western District of Washington



In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
11512 158th Avenue NE, Redmond, WA 98052, as)
described more particularly in Attachment A)

Case No. MJ24-309

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of Washington
(identify the person or describe the property to be searched and give its location):

11512 158th Avenue NE, Redmond, WA 98052, , as described more fully in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before June 4, 2024 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Any MJ of this District
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of .

Date and time issued: 5/22/24, 9:00 pm 1400

Judge's signature

City and state: Seattle, Washington

Michelle L. Peterson, United States Magistrate Judge

Printed name and title

Case No.:

Copy of warrant and inventory left with:

Inventory of the property taken and name of any person(s) seized:

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

The property to be searched is 11512 158th Ave NE, Redmond, WA 98052, further described as multi-story, single-family home, and any digital devices or other electronic storage media found therein. The street view and side view of the SUBJECT PREMISES are depicted in the following photographs:



ATTACHMENT B
ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. §§ 1349 (wire fraud conspiracy), 1343 (wire fraud), and 2 (aiding and abetting the same) (collectively, the “Subject Offenses”) involving Target Subject-1, ANTHONY CURCIO:

1. Evidence concerning occupancy or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys;

2. Trading cards and Pokémon cards located within the SUBJECT PREMISES;

3. Any tools, materials, and/or equipment that may be used to create forged card cases and labels;

4. For the time period of January 1, 2022 to the present, evidence relating to the Target Subjects communicating with victims, with each other, and with co-conspirators;

5. For the period of January 1, 2022 to the present, evidence of communications constituting or discussing or regarding the commission of the Subject Offenses;

6. Evidence concerning the identities and locations of co-conspirators and victims;

7. Evidence of criminal conduct, including communications reflecting an agreement between the Target Subjects and other co-conspirators to engage in the

1 scheme to defraud customers who purchased cards from the Target Subjects and their
2 co-conspirators;

3 8. Proceeds of the commission of the Subject Offenses, including any bulk
4 cash contained within the SUBJECT PREMISES;

5 9. Evidence of the use of aliases by the Target Subjects, including documents
6 reflecting false names;

7 10. Evidence relating to state of mind, including communications relating to
8 the Target Subjects' understanding that certain representations being made to
9 individuals purchasing cards from them were or must have been false;

10 11. For the time period of January 1, 2022 to the present, evidence of the
11 receipt, transfer, disposition or location of funds derived from the commission of the
12 Subject Offenses;

13 12. Records of Internet activity, including firewall logs, caches, browser history
14 and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered
15 into any Internet search engine, and records of user-typed web addresses;

16 13. Evidence of user attribution showing who used or owned an electronic
17 device at the time the things described in this warrant were created, edited, or deleted,
18 such as logs, phonebooks, saved usernames and passwords, documents, and browsing
19 history;

20 14. Any items or records needed to access the data stored on any seized or
21 copied electronic devices or storage media, including but not limited to any encryption
22 devices, or records of login credentials, passwords, private encryption keys, or similar
23 information;

24 15. Any items or records that may facilitate a forensic examination of
25 electronic devices or storage media, including any hardware or software manuals or
26 other information concerning the configuration of the seized or copied electronic
27 devices or storage media;

16. Location data, including but not limited to geolocation reporting and
location history data and metadata associated with other files that would place the
Target Subjects and any co-conspirators and/or aiders and abettors, as well as the
devices they used, in specific places at specific times, and would indicate the use of
their devices during those times;

17. Safes, key-lock strong boxes, suitcases, locked cabinets, and other types of
locked or closed containers used to secrete and store currency, electronic devices,
identification documents, books, records, financial instruments, and other and other

1 items within the categories described herein. Law enforcement agents executing this
 2 warrant are specifically authorized to open any such locked safes or containers
 3 including, where necessary, by using reasonable force. Law enforcement agents shall
 4 not seize locked safes or containers that do not contain evidence or fruits of the Subject
 5 Offenses, unless the safes or containers cannot be opened using reasonable force at the
 6 SUBJECT PREMISES. Any locked safe or container that can only be opened away
 7 from the SUBJECT PREMISES shall be returned if a later search shows that it does
 8 not contain evidence or fruits of the Subject Offenses;

9 18. Evidence concerning the location of other evidence of the Subject Offenses,
 10 including but not limited to information concerning addresses of other premises
 11 potentially containing relevant evidence, financial accounts where criminal proceeds
 12 may be stored, and communications reflecting registration of online accounts
 13 potentially containing relevant evidence;

14 19. Digital devices² or other electronic storage media³ that law enforcement
 15 reasonably suspects belong to Target Subject-1, ANTHONY CURCIO, containing any
 16 of the records or information described above or used as a means to commit the
 17 violations described above, including to generate, store, or transmit records in
 18 furtherance of the violations.

19 20. For any digital device or other electronic storage media upon which
 20 electronically stored information that is called for by this warrant may be contained,
 21 that may contain things otherwise called for by this warrant, or whose seizure is
 22 otherwise authorized by this warrant:

23 a. evidence of who used, owned, or controlled the digital device or
 24 other electronic storage media at the time the things described in this warrant were
 25 created, edited, or deleted, such as logs, registry entries, configuration files, saved
 26 usernames and passwords, documents, browsing history, user profiles, email, email
 27 contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital
 device or other electronic storage media, such as viruses, Trojan horses, and other forms

² "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

³ Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1 of malicious software, as well as evidence of the presence or absence of security software
2 designed to detect malicious software;

3 c. evidence of the lack of such malicious software;

4 d. evidence of the attachment to the digital device of other storage
5 devices or similar containers for electronic evidence;

6 e. evidence of counter-forensic programs (and associated data) that are
7 designed to eliminate data from the digital device or other electronic storage media;

8 f. evidence of the times the digital device or other electronic storage
9 media was used;

10 g. physical keys, encryption devices, dongles and similar physical
11 items that are necessary to gain access to the computer equipment, storage devices or
12 data; and

13 h. passwords, password files, test keys, encryption codes or other
14 information necessary to access the computer equipment, storage devices or data.

15 i. documentation and manuals that may be necessary to access the
16 digital device or other electronic storage media or to conduct a forensic examination of
17 the digital device or other electronic storage media;

18 j. applications, utility programs, compilers, interpreters, and other
19 software used to facilitate direct or indirect communication with the computer hardware,
20 storage devices, or data to be searched;

21 k. contextual information necessary to understand the evidence
22 described in this attachment.

23 THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE
24 MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS
25 SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO
26 THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC
27 STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL
ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE
CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR

1 EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED
2 CRIMES.

3 During the execution of the search of the SUBJECT PREMISES described in
4 Attachment A, if law enforcement encounters a smartphone or other electronic device
5 equipped with a biometric-unlock feature, and if law enforcement reasonably suspects
6 ANTHONY CURCIO is a user of the device, then – for the purpose of attempting to
7 unlock the device in order to search the contents as authorized by this warrant – law
8 enforcement personnel are authorized to: (1) press or swipe the fingers (including
9 thumbs) of CURCIO to the fingerprint scanner of the device; and/or (2) hold the device
10 in front of the face and open the eyes of CURCIO and activate the facial, iris, or retina
11 recognition feature.

12 In pressing or swiping an individual's thumb or finger onto a device and in
13 holding a device in front of an individual's face and open eyes, law enforcement may not
14 use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically,
15 law enforcement may use no more than objectively reasonable force in light of the facts
16 and circumstances confronting them.

17
18
19
20
21
22
23
24
25
26
27

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Collected Item Log

Event Title: (U) Seizure of Evidence Items from 11512 158th Ave NE, Redmond, WA **Date:** 05/30/2024

Approved By: A/SSA Gregory L. Leiman

Drafted By: BENESH DANIELLE LYNN

Case ID #: 87N-NY-3740727 (U) OPERATION HEIST AND HOLDER; Anthony Curcio, Joe Bondarchuk, Jason Donley; PSA - Victim; ITSP

Enclosure(s): Enclosed are the following items:

1. (U) Evidence Recovery Log

Details:

A search warrant, issued in the United States District Court for the Western District of Washington on May 22, 2024, was executed by the members of FBI Seattle on May 23, 2024.

The search warrant approved the seizure of evidence related to violations of 18 U.S.C. Section 1349(wire fraud conspiracy), 1343 (wire fraud), and 2(aiding and abetting the same). The following items were seized from the residence of subject Anthony Curcio at 11512 158th Avenue NE, Redmond, Washington 98052.

Collected From: (U) Anthony Curcio and Emily Curcio
11512 158th Avenue NE
Redmond , Washington 98052
United States

Receipt Given?: Yes

Holding Office: SE - SEATTLE

UNCLASSIFIED

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

UNCLASSIFIED

Title: (U) Seizure of Evidence Items from 11512 158th Ave NE, Redmond, WA

Re: 87N-NY-3740727, 05/30/2024

Item Type	Description
1B General	(U) Binder of Trading Cards Collected On: 05/23/2024 02:20 PM EDT Seizing Individual: BENESH DANIELLE LYNN Located By: Lexis Pawlowski Other Locator: Grant Knorr Location Area: Room A: Ground-Floor Bedroom Specific Location: Floor
1B General	(U) Tackle-box of Tools Collected On: 05/23/2024 02:20 PM EDT Seizing Individual: BENESH DANIELLE LYNN Located By: Lexis Pawlowski Other Locator: Nike Kline Location Area: Room A: Ground-Floor Bedroom Specific Location: Floor
1B General	(U) Finished Trading Cards Collected On: 05/23/2024 02:20 PM EDT Seizing Individual: BENESH DANIELLE LYNN Located By: Lexis Pawlowski Other Locator: Grant Knorr Location Area: Room A: Ground-Floor Bedroom Specific Location: Floor
1B General	(U) Card Packaging Material Collected On: 05/23/2024 02:20 PM EDT Seizing Individual: BENESH DANIELLE LYNN Located By: Lexis Pawlowski Other Locator: Nick Kline Location Area: Room A: Ground-Floor Bedroom Specific Location: Floor
1B General	(U) Box of Packaging and Tools Collected On: 05/23/2024 02:20 PM EDT Seizing Individual: BENESH DANIELLE LYNN Located By: Lexis Pawlowski Other Locator: Nick Kline Location Area: Room A: Ground-Floor Bedroom

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Seizure of Evidence Items from 11512 158th Ave NE, Redmond, WA

Re: 87N-NY-3740727, 05/30/2024

Specific Location: Floor

1B General (U) Trading Card Packaging
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: Floor

1B General (U) Trading Cards in Cases
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: Floor

1B General (U) 3-D Printer
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: Floor

1B Digital (U) Sandisk 16GB USB Drive
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: In 3-D Printer
Device Type: USB Micro Storage Device (thumb drive)
Make: Sandisk
Data Capacity: 16GB
Number of Devices Collected: 1

1B General (U) Assorted Trading Cards

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Seizure of Evidence Items from 11512 158th Ave NE, Redmond, WA

Re: 87N-NY-3740727, 05/30/2024

Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: Floor

1B General (U) Label Printer in Container
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: Floor

1B General (U) Container with Labels
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: Floor

1B General (U) Ryobi Buffing Drill, Soldering Iron
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: Floor

1B General (U) Target bag with Trading Card Containers
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: Under desk

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Seizure of Evidence Items from 11512 158th Ave NE, Redmond, WA

Re: 87N-NY-3740727, 05/30/2024

1B General (U) Trading Cards in Cases
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: On desk

1B General (U) Empty Card Containers
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom

1B General (U) Loose Card Labels
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: On desk

1B General (U) 2 Trading Cards Not in Containers
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Nick Kline
Location Area: Room A: Ground-Floor Bedroom
Specific Location: Top desk drawer

1B Digital (U) Black Apple MacBook Pro, A1990
Serial Number: C02Y91W1JGH6
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: In Backpack
Device Type: Laptop/Tablet Computer

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Seizure of Evidence Items from 11512 158th Ave NE, Redmond, WA

Re: 87N-NY-3740727, 05/30/2024

Make: Apple
Model: A1990
Serial Number: C02Y91W1JGH6
Number of Devices Collected: 1

1B Digital (U) Sandisk Portable SSDs
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: In black backpack
Device Type: SD Card
Make: Sandisk
Number of Devices Collected: 4

1B Digital (U) Adata SD Cards
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: In black backpack
Device Type: SD Card
Make: Adata
Number of Devices Collected: 2

1B General (U) Bauer Dremel Tool
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: On floor in black duffel bag

1B General (U) Portable Label Maker and Accessories
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Ethan A. Via
Other Locator: Adam Roeser

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Seizure of Evidence Items from 11512 158th Ave NE, Redmond, WA

Re: 87N-NY-3740727, 05/30/2024

Location Area: Room F: Garage
Specific Location: On floor

1B General (U) Curcio Media Stamp
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room C: Closet in Ground-Floor Bathroom
Specific Location: Shelf above computer monitor

1B General (U) Handwritten Notes
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room C: Closet in Ground-Floor Bathroom
Specific Location: On shelf

1B General (U) Acetone
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom
Specific Location: On shelf

1B General (U) Liquid Resin Components
Collected On: 05/23/2024 02:20 PM EDT
Seizing Individual: BENESH DANIELLE LYNN
Located By: Lexis Pawlowski
Other Locator: Grant Knorr
Location Area: Room A: Ground-Floor Bedroom

◆◆

UNCLASSIFIED